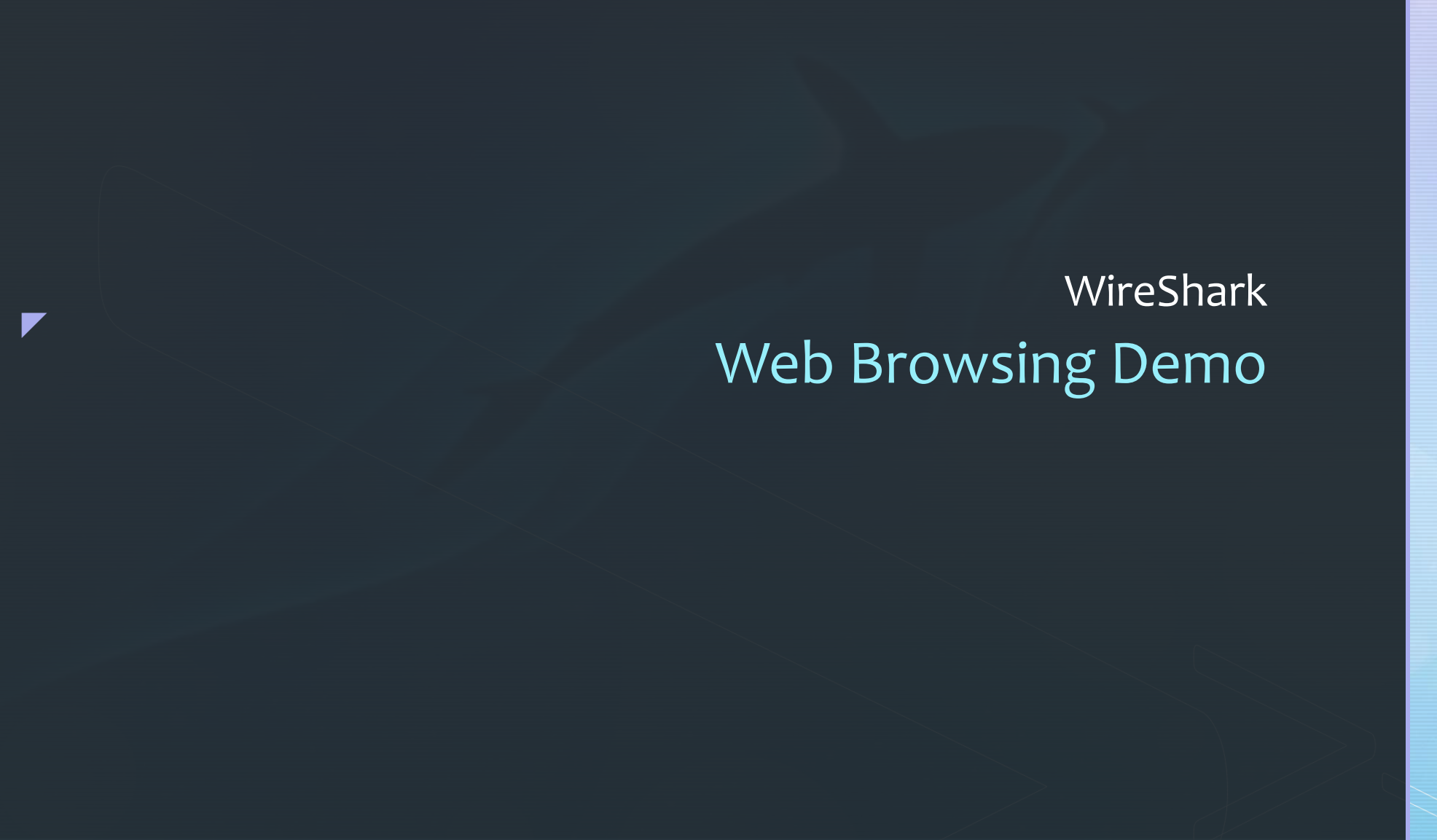


Δρ. Άννα Κεφάλα



WireShark (a network protocol analyser)



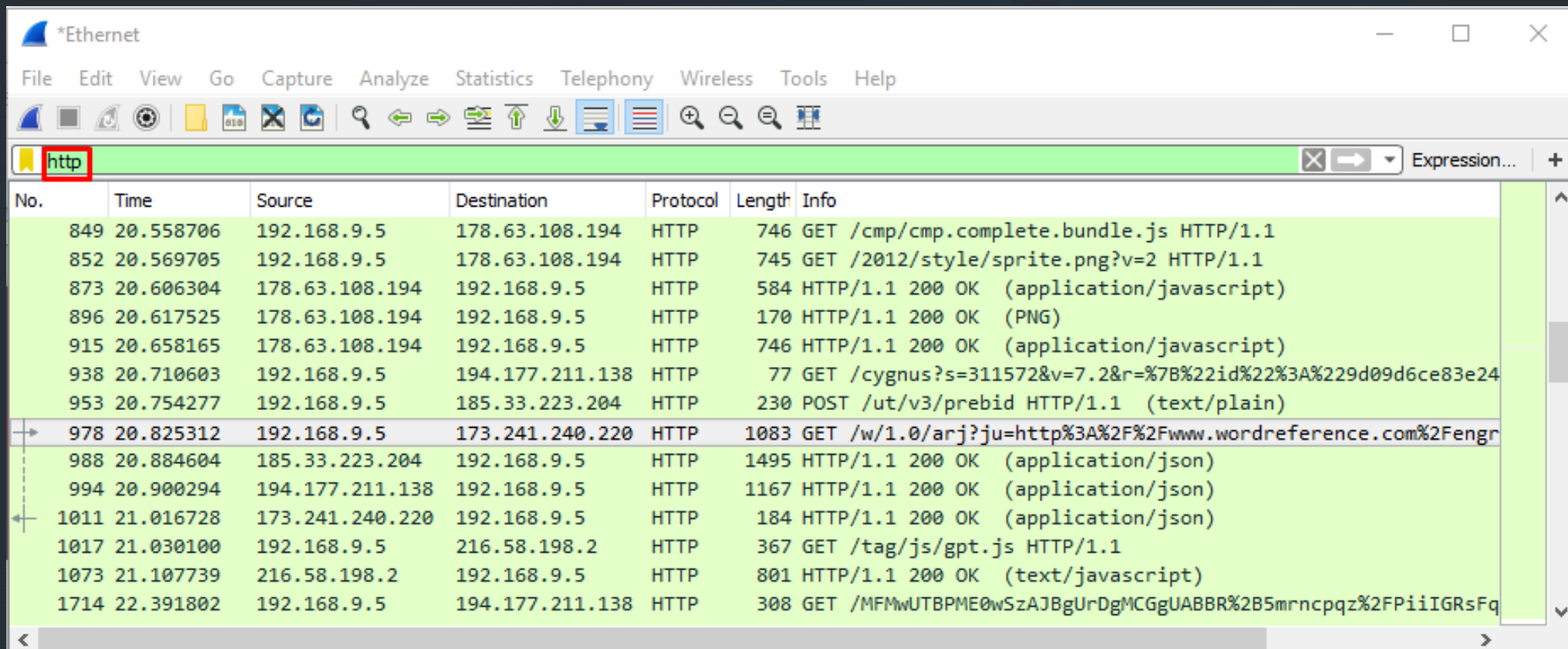
WireShark Web Browsing Demo

Try it out!

- Ξεκινήστε τον Browser
- Ξεκινήστε το WireShark
- Επιλέξτε το interface για ανίχνευση
- Ξεκινήστε την ανίχνευση 
- Visit <http://ccslab.aueb.gr/> ή κάποιο άλλο URL
- Σταματήστε την ανίχνευση 
- Ανάμεσα στα πακέτα που ανιχνεύθηκαν υπάρχει και η ανταλλαγή των HTTP μηνυμάτων...

Filtering

Filter HTTP κίνηση



The image shows a Wireshark packet capture window titled "*Ethernet". The filter bar at the top contains the filter "http". The packet list below shows several HTTP packets. The packet at sequence number 978 is highlighted, showing a GET request to a WordReference URL.

No.	Time	Source	Destination	Protocol	Length	Info
849	20.558706	192.168.9.5	178.63.108.194	HTTP	746	GET /cmp/cmp.complete.bundle.js HTTP/1.1
852	20.569705	192.168.9.5	178.63.108.194	HTTP	745	GET /2012/style/sprite.png?v=2 HTTP/1.1
873	20.606304	178.63.108.194	192.168.9.5	HTTP	584	HTTP/1.1 200 OK (application/javascript)
896	20.617525	178.63.108.194	192.168.9.5	HTTP	170	HTTP/1.1 200 OK (PNG)
915	20.658165	178.63.108.194	192.168.9.5	HTTP	746	HTTP/1.1 200 OK (application/javascript)
938	20.710603	192.168.9.5	194.177.211.138	HTTP	77	GET /cygnus?s=311572&v=7.2&r=%7B%22id%22%3A%229d09d6ce83e24
953	20.754277	192.168.9.5	185.33.223.204	HTTP	230	POST /ut/v3/prebid HTTP/1.1 (text/plain)
978	20.825312	192.168.9.5	173.241.240.220	HTTP	1083	GET /w/1.0/arj?ju=http%3A%2F%2Fwww.wordreference.com%2Fengr
988	20.884604	185.33.223.204	192.168.9.5	HTTP	1495	HTTP/1.1 200 OK (application/json)
994	20.900294	194.177.211.138	192.168.9.5	HTTP	1167	HTTP/1.1 200 OK (application/json)
1011	21.016728	173.241.240.220	192.168.9.5	HTTP	184	HTTP/1.1 200 OK (application/json)
1017	21.030100	192.168.9.5	216.58.198.2	HTTP	367	GET /tag/js/gpt.js HTTP/1.1
1073	21.107739	216.58.198.2	192.168.9.5	HTTP	801	HTTP/1.1 200 OK (text/javascript)
1714	22.391802	192.168.9.5	194.177.211.138	HTTP	308	GET /MFMwUTBPME0wSzAJBgUrDgMCGgUABBR%2B5mrncpqz%2FPiiIGRsFq

Analyzing

- Επιλέξτε ένα HTTP GET πακέτο

The image shows a Wireshark packet capture window titled "*Ethernet". The packet list pane displays several HTTP packets. Packet 978 is highlighted with a red box, indicating it is the selected packet. The packet details pane shows the structure of the selected packet, including the Ethernet II header, Internet Protocol Version 4 header, Transmission Control Protocol header, and Hypertext Transfer Protocol header. The packet bytes pane shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
849	20.558706	192.168.9.5	178.63.108.194	HTTP	746	GET /cmp/cmp.complete.bundle.js HTTP/1.1
852	20.569705	192.168.9.5	178.63.108.194	HTTP	745	GET /2012/style/sprite.png?v=2 HTTP/1.1
873	20.606304	178.63.108.194	192.168.9.5	HTTP	584	HTTP/1.1 200 OK (application/javascript)
896	20.617525	178.63.108.194	192.168.9.5	HTTP	170	HTTP/1.1 200 OK (PNG)
915	20.658165	178.63.108.194	192.168.9.5	HTTP	746	HTTP/1.1 200 OK (application/javascript)
938	20.710603	192.168.9.5	194.177.211.138	HTTP	77	GET /cygnus?s=311572&v=7.2&r=%7B%22id%22%3A%2229d09d6ce83e246%
953	20.754277	192.168.9.5	185.33.223.204	HTTP	230	POST /ut/v3/prebid HTTP/1.1 (text/plain)
978	20.825312	192.168.9.5	173.241.240.220	HTTP	1083	GET /w/1.0/arj?ju=http%3A%2F%2Fwww.wordreference.com%2Fengr%2
988	20.884604	185.33.223.204	192.168.9.5	HTTP	1495	HTTP/1.1 200 OK (application/json)
994	20.900294	194.177.211.138	192.168.9.5	HTTP	1167	HTTP/1.1 200 OK (application/json)
1011	21.016728	173.241.240.220	192.168.9.5	HTTP	184	HTTP/1.1 200 OK (application/json)
1017	21.030100	192.168.9.5	216.58.198.2	HTTP	367	GET /tag/js/gpt.js HTTP/1.1
1073	21.107730	216.58.198.2	192.168.9.5	HTTP	801	HTTP/1.1 200 OK (text/javascript)

Frame 978: 1083 bytes on wire (8664 bits), 1083 bytes captured (8664 bits) on interface 0
 > Ethernet II, Src: Giga-Byt_48:19:9f (fc:aa:14:48:19:9f), Dst: Fortinet_09:00:25 (00:09:0f:09:00:25)
 > Internet Protocol Version 4, Src: 192.168.9.5, Dst: 173.241.240.220
 > Transmission Control Protocol, Src Port: 54334, Dst Port: 80, Seq: 1, Ack: 1, Len: 1029
 > Hypertext Transfer Protocol

0030 01 00 54 ef 00 00 47 45 54 20 2f 77 2f 31 2e 30 ..T...GET /w/1.0
 0040 2f 61 72 6a 3f 6a 75 3d 68 74 74 70 25 33 41 25 /arj?ju= http%3A%
 0050 32 46 25 32 46 77 77 77 2e 77 6f 72 64 72 65 66 2F%2Fwww .wordref
 0060 65 72 65 6e 63 65 2e 63 6f 6d 25 32 46 65 6e 67 erence.c om%2Feng

Hypertext Transfer Protocol (http), 1029 bytes | Packets: 3551 · Displayed: 67 (1.9%) · Dropped: 0 (0.0%) | Profile: Default

- Communicating peers

Analyzing IP

The image shows a Wireshark packet capture window titled "*Ethernet". The packet list pane shows several HTTP packets. Packet 978 is selected, showing details of an HTTP GET request. The packet is 1083 bytes long, captured on interface 0. The source IP is 192.168.9.5 and the destination IP is 173.241.240.220. The packet is an Internet Protocol Version 4 (IPv4) packet with a version of 4, header length of 20 bytes, and a total length of 1069 bytes. The differentiated services field is 0x00 (DSCP: CS0, ECN: Not-ECT). The total length is 1069 bytes. The identification is 0x187f (6271). The flags are 0x4000, Don't fragment. The time to live is 128. The protocol is TCP (6). The header checksum is 0x75d0 [validation disabled]. The header checksum status is Unverified. The source is 192.168.9.5 and the destination is 173.241.240.220. The transmission control protocol details show the source port is 54334, destination port is 80, sequence number is 1, acknowledgment number is 1, and length is 1029 bytes. The packet bytes pane shows the raw data of the HTTP GET request, including the method, URI, and headers.

No.	Time	Source	Destination	Protocol	Length	Info
896	20.617525	178.63.108.194	192.168.9.5	HTTP	170	HTTP/1.1 200 OK (PNG)
915	20.658165	178.63.108.194	192.168.9.5	HTTP	746	HTTP/1.1 200 OK (application/javascript)
938	20.710603	192.168.9.5	194.177.211.138	HTTP	77	GET /cygnus?s=311572&v=7.2&r=%7B%22id%22%3A%229d09d6ce83e246%
953	20.754277	192.168.9.5	185.33.223.204	HTTP	230	POST /ut/v3/prebid HTTP/1.1 (text/plain)
978	20.825312	192.168.9.5	173.241.240.220	HTTP	1083	GET /w/1.0/arj?ju=http%3A%2F%2Fwww.wordreference.com%2Fengr%2
988	20.884604	185.33.223.204	192.168.9.5	HTTP	1495	HTTP/1.1 200 OK (application/json)
994	20.900294	194.177.211.138	192.168.9.5	HTTP	1167	HTTP/1.1 200 OK (application/json)
1011	21.016728	173.241.240.220	192.168.9.5	HTTP	184	HTTP/1.1 200 OK (application/json)

Frame 978: 1083 bytes on wire (8664 bits), 1083 bytes captured (8664 bits) on interface 0
 Ethernet II, Src: Giga-Byt_48:19:9f (fc:aa:14:48:19:9f), Dst: Fortinet_09:00:25 (00:09:0f:09:00:25)
 Internet Protocol Version 4, Src: 192.168.9.5, Dst: 173.241.240.220
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 1069
 Identification: 0x187f (6271)
 Flags: 0x4000, Don't fragment
 Time to live: 128
 Protocol: TCP (6)
 Header checksum: 0x75d0 [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.9.5
 Destination: 173.241.240.220
 Transmission Control Protocol, Src Port: 54334, Dst Port: 80, Seq: 1, Ack: 1, Len: 1029
 0030 01 00 54 ef 00 00 47 45 54 20 2f 77 2f 31 2e 30 ..T...GE T /w/1.0
 0040 2f 61 72 6a 3f 6a 75 3d 68 74 74 70 25 33 41 25 /arj?ju= http%3A%
 0050 32 46 25 32 46 77 77 77 2e 77 6f 72 64 72 65 66 2F%2Fwww .wordref
 0060 65 72 65 6e 63 65 2e 63 6f 6d 25 32 46 65 6e 67 erence.c om%2Feng
 0070 72 25 32 46 6c 6f 6f 6b 25 32 35 32 30 66 6f 72 r%2Flook %2520for

Hypertext Transfer Protocol (http), 1029 bytes | Packets: 3551 · Displayed: 67 (1.9%) · Dropped: 0 (0.0%) | Profile: Default

Analyzing Transportation Level

- TCP, well-known port for HTTP?

The image shows a Wireshark packet capture window titled "*Ethernet". The packet list on the left shows several HTTP packets. Packet 978 is selected, showing a GET request to `/w/1.0/arj?ju=http%3A%2F%2Fwww.wordreference.com%2Fengr%2Flook%2520for`. The packet details pane on the right shows the structure of the packet, including the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol (TCP) header. The TCP header shows the destination port as 80, which is highlighted with a red box. The packet bytes pane at the bottom shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
896	20.617525	178.63.108.194	192.168.9.5	HTTP	170	HTTP/1.1 200 OK (PNG)
915	20.658165	178.63.108.194	192.168.9.5	HTTP	746	HTTP/1.1 200 OK (application/javascript)
938	20.710603	192.168.9.5	194.177.211.138	HTTP	77	GET /cygnus?s=311572&v=7.2&r=%7B%22id%22%3A%229d09d6ce83e246%
953	20.754277	192.168.9.5	185.33.223.204	HTTP	230	POST /ut/v3/prebid HTTP/1.1 (text/plain)
978	20.825312	192.168.9.5	173.241.240.220	HTTP	1083	GET /w/1.0/arj?ju=http%3A%2F%2Fwww.wordreference.com%2Fengr%2Flook%2520for
988	20.884604	185.33.223.204	192.168.9.5	HTTP	1495	HTTP/1.1 200 OK (application/json)
994	20.900294	194.177.211.138	192.168.9.5	HTTP	1167	HTTP/1.1 200 OK (application/json)
1011	21.016728	173.241.240.220	192.168.9.5	HTTP	184	HTTP/1.1 200 OK (application/json)

Frame 978: 1083 bytes on wire (8664 bits), 1083 bytes captured (8664 bits) on interface 0

Ethernet II, Src: Giga-Byt_48:19:9f (fc:aa:14:48:19:9f), Dst: Fortinet_09:00:25 (00:09:0f:09:00:25)

Internet Protocol Version 4, Src: 192.168.9.5, Dst: 173.241.240.220

Transmission Control Protocol, Src Port: 54334, Dst Port: 80, Seq: 1, Ack: 1, Len: 1029

Source Port: 54334

Destination Port: 80

[Stream index: 32]

[TCP Segment Len: 1029]

Sequence number: 1 (relative sequence number)

[Next sequence number: 1030 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

0101 = Header Length: 20 bytes (5)

Flags: 0x018 (PSH, ACK)

Window size value: 256

[Calculated window size: 65536]

[Window size scaling factor: 256]

0030 01 00 54 ef 00 00 47 45 54 20 2f 77 2f 31 2e 30 ..T...GE T /w/1.0

0040 2f 61 72 6a 3f 6a 75 3d 68 74 74 70 25 33 41 25 /arj?ju= http%3A%

0050 32 46 25 32 46 77 77 77 2e 77 6f 72 64 72 65 66 2F%2Fwww .wordref

0060 65 72 65 6e 63 65 2e 63 6f 6d 25 32 46 65 6e 67 erence.c om%2Feng

0070 72 25 32 46 6c 6f 6f 6b 25 32 35 32 30 66 6f 72 r%2Flook %2520for

Hypertext Transfer Protocol (http), 1029 bytes

Packets: 3551 · Displayed: 67 (1.9%) · Dropped: 0 (0.0%) Profile: Default

Analyzing HTTP GET message

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
953	20.754277	192.168.9.5	185.33.223.204	HTTP	230	POST /ut/v3/prebid HTTP/1.1 (text/plain)
978	20.825312	192.168.9.5	173.241.240.220	HTTP	1083	GET /w/1.0/arj?ju=http%3A%2F%2Fwww.wordreference.com%2Fengr%2
988	20.884604	185.33.223.204	192.168.9.5	HTTP	1495	HTTP/1.1 200 OK (application/json)
994	20.900294	194.177.211.138	192.168.9.5	HTTP	1167	HTTP/1.1 200 OK (application/json)
1011	21.016728	173.241.240.220	192.168.9.5	HTTP	184	HTTP/1.1 200 OK (application/json)
1017	21.030100	192.168.9.5	216.58.198.2	HTTP	367	GET /tag/is/gpt.is HTTP/1.1

> Frame 978: 1083 bytes on wire (8664 bits), 1083 bytes captured (8664 bits) on interface 0

> Ethernet II, Src: Giga-Byt_48:19:9f (fc:aa:14:48:19:9f), Dst: Fortinet_09:00:25 (00:09:0f:09:00:25)

> Internet Protocol Version 4, Src: 192.168.9.5, Dst: 173.241.240.220

> Transmission Control Protocol, Src Port: 54334, Dst Port: 80, Seq: 1, Ack: 1, Len: 1029

> Hypertext Transfer Protocol

> [truncated]GET /w/1.0/arj?ju=http%3A%2F%2Fwww.wordreference.com%2Fengr%2Flook%2520for&jr=http%3A%2F%2Fwww.wordreference.com%2...

Host: wordreference-d.openx.net\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0\r\n

Accept: */*\r\n

Accept-Language: en-US,en;q=0.5\r\n

Accept-Encoding: gzip, deflate\r\n

Referer: http://www.wordreference.com/engr/look%20for\r\n

Content-Type: text/plain\r\n

Origin: http://www.wordreference.com\r\n

Connection: keep-alive\r\n

> Cookie: i=bbc7b46b-1d73-4c88-2250-44f0bed7a473|1441350232; p_synced=j0.pp.ph.oX.px.pw.oL.jQ.oT.ma.im.ie.mS.pF.ns.t9.ku.qH.sj; ... \r\n

[Full request URI [truncated]: http://wordreference-d.openx.net/w/1.0/arj?ju=http%3A%2F%2Fwww.wordreference.com%2Fengr%2Flook%...

[HTTP request 1/1]

[Response in frame: 1011]

Analyzing HTTP response message

The image shows a Wireshark packet capture window titled '*Ethernet'. The packet list on the left shows several HTTP packets. Packet 1011 is selected, showing an HTTP 200 OK response from 173.241.240.220 to 192.168.9.5. The packet details pane on the right shows the structure of the response, including the status line, headers, and body. The 'Server' header is highlighted with a red box, showing 'OXGW/16.103.1'. The 'Request in frame: 978' is highlighted with a green box at the bottom.

No.	Time	Source	Destination	Protocol	Length	Info
953	20.754277	192.168.9.5	185.33.223.204	HTTP	230	POST /ut/v3/prebid HTTP/1.1 (text/plain)
978	20.825312	192.168.9.5	173.241.240.220	HTTP	1083	GET /w/1.0/arj?ju=http%3A%2F%2Fwww.wordreference.com%2Fengr%2
988	20.884604	185.33.223.204	192.168.9.5	HTTP	1495	HTTP/1.1 200 OK (application/json)
994	20.900294	194.177.211.138	192.168.9.5	HTTP	1167	HTTP/1.1 200 OK (application/json)
1011	21.016728	173.241.240.220	192.168.9.5	HTTP	184	HTTP/1.1 200 OK (application/json)
1017	21.030100	192.168.9.5	216.58.198.2	HTTP	367	GET /tao/is/ent is HTTP/1.1

Frame 1011: 184 bytes on wire (1472 bits), 184 bytes captured (1472 bits) on interface 0
 Ethernet II, Src: Fortinet_09:00:25 (00:09:0f:09:00:25), Dst: Giga-Byt_48:19:9f (fc:aa:14:48:19:9f)
 Internet Protocol Version 4, Src: 173.241.240.220, Dst: 192.168.9.5
 Transmission Control Protocol, Src Port: 80, Dst Port: 54334, Seq: 4381, Ack: 1030, Len: 130
 [4 Reassembled TCP Segments (4510 bytes): #1007(1460), #1009(1460), #1010(1460), #1011(130)]
 Hypertext Transfer Protocol
 HTTP/1.1 200 OK\r\n
 Vary: Accept\r\n
 Set-Cookie: p_synced=j0.pp.ph.oX.px.pw.oL.jQ.oT.ma.im.ie.mS.pF.ns.t9.ku.qH.sj; Version=1; Expires=Wed, 21-Nov-2018 14:50:21 GM
 Set-Cookie: i=bbc7b46b-1d73-4c88-2250-44f0bed7a473|1441350232; Version=1; Expires=Wed, 06-Nov-2019 14:50:21 GMT; Max-Age=31536
 Server: OXGW/16.103.1\r\n
 Pragma: no-cache\r\n
 P3P: CP="CUR ADM OUR NOR STA NID"\r\n
 Expires: Mon, 26 Jul 1997 05:00:00 GMT\r\n
 Date: Tue, 06 Nov 2018 14:50:21 GMT\r\n
 Content-Type: application/json\r\n
 Cache-Control: private, max-age=0, no-cache\r\n
 Access-Control-Allow-Origin: http://www.wordreference.com\r\n
 Access-Control-Allow-Credentials: true\r\n
 Transfer-Encoding: chunked\r\n
 Content-Encoding: gzip\r\n
 \r\n
 [HTTP response 1/1]
 [Time since request: 0.191416000 seconds]
 [Request in frame: 978]

Wireshark

FTP (File Transfer Protocol) Demo

Try it out!

- Ξεκινήστε το Wireshark
- Επιλέξτε το interface για ανίχνευση
- Ξεκινήστε την ανίχνευση 
- Ανοίξτε ένα command-line παράθυρο

FTP command-line

- ftp ftp.hellug.gr (user: anonymous, pass: email address)

```
Command Prompt - ftp ftp.hellug.gr
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

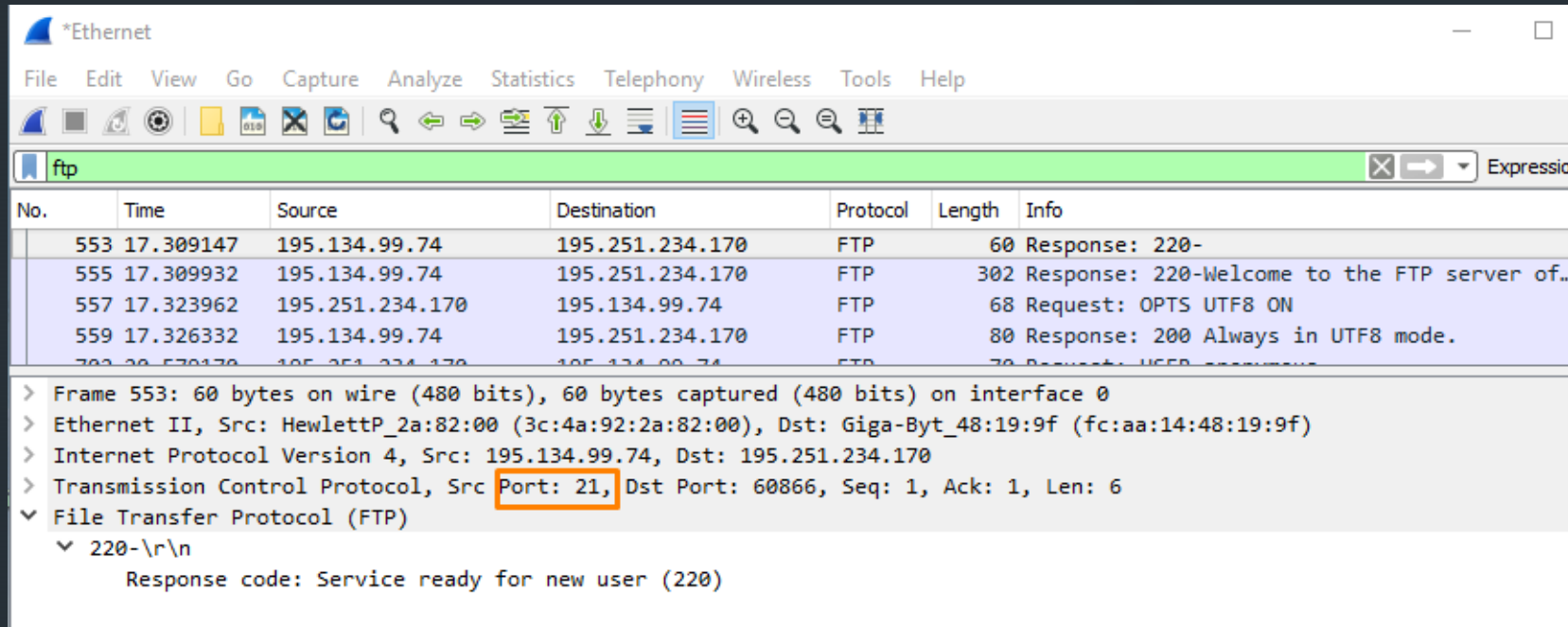
C:\Users\anna>ftp ftp.hellug.gr
Connected to tux-cave.hellug.gr.
220-
220-Welcome to the FTP server of HEL.L.U.G. (http://www.hellug.gr)
220-
220-Contact ftpadmin[*] for problems and/or suggestions.
220-
220-[*] contact address is at hellug dot gr domain,
220-   username as you see it above
220-
200 Always in UTF8 mode.
User (tux-cave.hellug.gr:(none)): anonymous
331 Please specify the password.
Password:
230 Login successful.
ftp>
```

FTP | Get a file

- cd pub/gnutls (change directory)
- get README (file)
- stop capturing

```
ftp>  
ftp> cd pub/gnutls  
250-More information on GnuTLS can be found at http://www.gnutls.org/  
250-  
250 Directory successfully changed.  
ftp> get README  
200 PORT command successful. Consider using PASV.  
150 Opening BINARY mode data connection for README (67 bytes).  
226 Transfer complete.  
ftp: 67 bytes received in 0.00Seconds 67000.00Kbytes/sec.  
ftp>
```

Filter: ftp

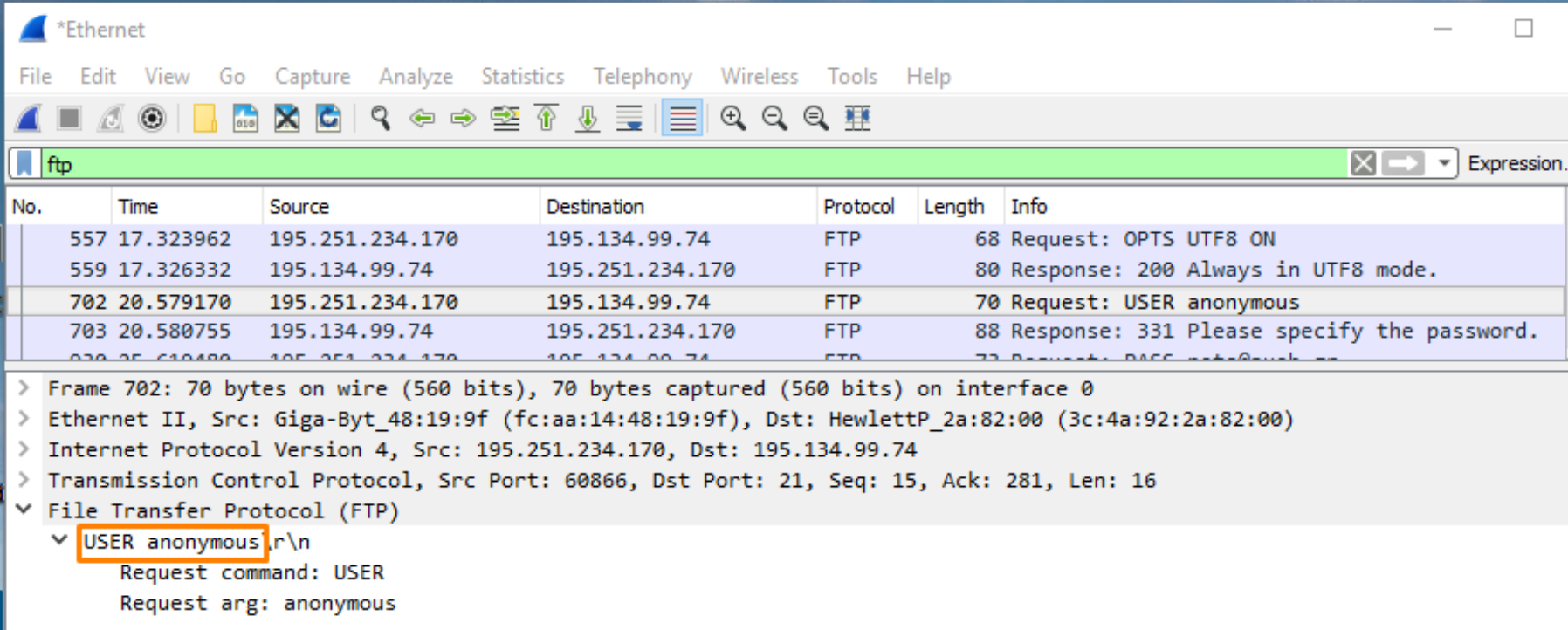


The image shows a Wireshark packet capture window titled "*Ethernet". The filter bar at the top contains the text "ftp". Below the filter bar, a list of captured packets is displayed. The selected packet is number 553, which is an FTP response. The packet details pane on the right shows the following information:

- Frame 553: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
- Ethernet II, Src: HewlettP_2a:82:00 (3c:4a:92:2a:82:00), Dst: Giga-Byt_48:19:9f (fc:aa:14:48:19:9f)
- Internet Protocol Version 4, Src: 195.134.99.74, Dst: 195.251.234.170
- Transmission Control Protocol, Src Port: 21, Dst Port: 60866, Seq: 1, Ack: 1, Len: 6
- File Transfer Protocol (FTP)
 - 220-\r\n
 - Response code: Service ready for new user (220)

TCP port 21
(well known)

FTP login: username



The screenshot displays the Wireshark network protocol analyzer interface. The packet list pane shows several captured packets, with frame 702 selected. The packet details pane for frame 702 is expanded, showing the File Transfer Protocol (FTP) layer. The 'USER anonymous' request is highlighted with an orange box, indicating the username used for login.

No.	Time	Source	Destination	Protocol	Length	Info
557	17.323962	195.251.234.170	195.134.99.74	FTP	68	Request: OPTS UTF8 ON
559	17.326332	195.134.99.74	195.251.234.170	FTP	80	Response: 200 Always in UTF8 mode.
702	20.579170	195.251.234.170	195.134.99.74	FTP	70	Request: USER anonymous
703	20.580755	195.134.99.74	195.251.234.170	FTP	88	Response: 331 Please specify the password.

Frame 702: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0

- Ethernet II, Src: Giga-Byt_48:19:9f (fc:aa:14:48:19:9f), Dst: HewlettP_2a:82:00 (3c:4a:92:2a:82:00)
- Internet Protocol Version 4, Src: 195.251.234.170, Dst: 195.134.99.74
- Transmission Control Protocol, Src Port: 60866, Dst Port: 21, Seq: 15, Ack: 281, Len: 16
- File Transfer Protocol (FTP)
 - USER anonymous\r\n
 - Request command: USER
 - Request arg: anonymous

FTP login: *password* (clear text)

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ftp

No.	Time	Source	Destination	Protocol	Length	Info
559	17.326332	195.134.99.74	195.251.234.170	FTP	80	Response: 200 Always in UTF8 mode.
702	20.579170	195.251.234.170	195.134.99.74	FTP	70	Request: USER anonymous
703	20.580755	195.134.99.74	195.251.234.170	FTP	88	Response: 331 Please specify the password.
930	25.619480	195.251.234.170	195.134.99.74	FTP	73	Request: PASS nets@aueb.gr

> Frame 703: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface 0

> Ethernet II, Src: HewlettP_2a:82:00 (3c:4a:92:2a:82:00), Dst: Giga-Byt_48:19:9f (fc:aa:14:48:19:9f)

> Internet Protocol Version 4, Src: 195.134.99.74, Dst: 195.251.234.170

> Transmission Control Protocol, Src Port: 21, Dst Port: 60866, Seq: 281, Ack: 31, Len: 34

> File Transfer Protocol (FTP)

> 331 Please specify the password.\r\n

Response code: User name okay, need password (331)

Response arg: Please specify the password.

Password is intercepted!!!

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ftp

No.	Time	Source	Destination	Protocol	Length	Info
559	17.326332	195.134.99.74	195.251.234.170	FTP	80	Response: 200 Always in UTF8 mode.
702	20.579170	195.251.234.170	195.134.99.74	FTP	70	Request: USER anonymous
703	20.580755	195.134.99.74	195.251.234.170	FTP	88	Response: 331 Please specify the password.
930	25.619480	195.251.234.170	195.134.99.74	FTP	73	Request: PASS nets@aueb.gr

> Frame 930: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0

> Ethernet II, Src: Giga-Byt_48:19:9f (fc:aa:14:48:19:9f), Dst: HewlettP_2a:82:00 (3c:4a:92:2a:82:00)

> Internet Protocol Version 4, Src: 195.251.234.170, Dst: 195.134.99.74

> Transmission Control Protocol, Src Port: 60866, Dst Port: 21, Seq: 31, Ack: 315, Len: 19

> File Transfer Protocol (FTP)

> PASS nets@aueb.gr\r\n

Request command: PASS

Request arg: nets@aueb.gr

Retrieve file commands

FTP Protocol

```

v File Transfer Protocol (FTP)
  v 200 PORT command successful. Consider using PASV.\r\n
    Response code: Command okay (200)
    Response arg: PORT command successful. Consider using PASV.
  
```

```

> Internet Protocol Version 4, Src: 195.251.234.170, Dst: 195.134.99.74
> Transmission Control Protocol, Src Port: 60866, Dst Port: 21, Seq: 96, Ack: 503, Len: 13
v File Transfer Protocol (FTP)
  v RETR README\r\n
    Request command: RETR
    Request arg: README
  
```

```

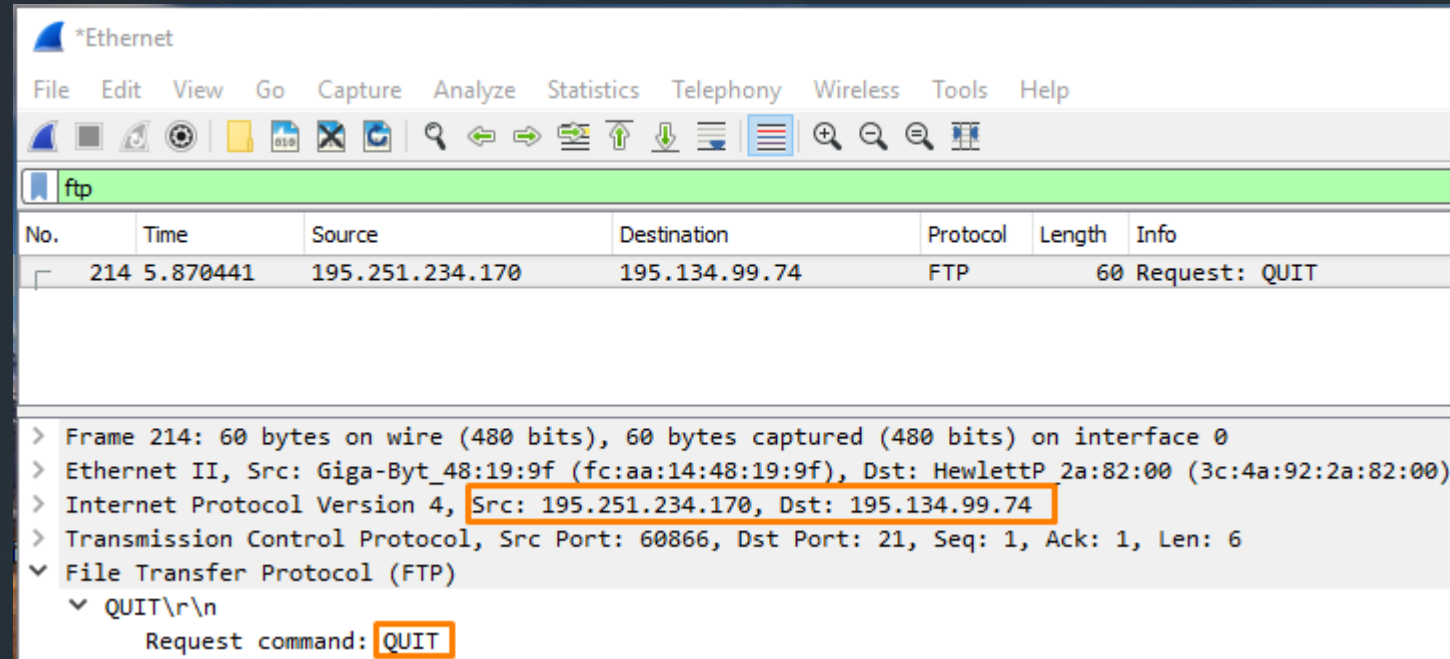
> Internet Protocol Version 4, Src: 195.134.99.74, Dst: 195.251.234.170
> Transmission Control Protocol, Src Port: 21, Dst Port: 60866, Seq: 503, Ack: 109, Len: 64
v File Transfer Protocol (FTP)
  v 150 Opening BINARY mode data connection for README (67 bytes).\r\n
    Response code: File status okay; about to open data connection (150)
    Response arg: Opening BINARY mode data connection for README (67 bytes).
  
```

```

> Internet Protocol Version 4, Src: 195.134.99.74, Dst: 195.251.234.170
> Transmission Control Protocol, Src Port: 21, Dst Port: 60866, Seq: 567, Ack: 109, Len: 24
v File Transfer Protocol (FTP)
  v 226 Transfer complete.\r\n
    Response code: Closing data connection (226)
    Response arg: Transfer complete.
  
```

Quit the session

```
ftp> close
421 timeout.
ftp> bye
```



The image shows a Wireshark packet capture window titled '*Ethernet'. The packet list pane shows a single packet, No. 214, at time 5.870441, from source 195.251.234.170 to destination 195.134.99.74, protocol FTP, length 60, with info 'Request: QUIT'. The packet details pane shows the following structure:

- > Frame 214: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
- > Ethernet II, Src: Giga-Byt_48:19:9f (fc:aa:14:48:19:9f), Dst: HewlettP 2a:82:00 (3c:4a:92:2a:82:00)
- > Internet Protocol Version 4, Src: 195.251.234.170, Dst: 195.134.99.74
- > Transmission Control Protocol, Src Port: 60866, Dst Port: 21, Seq: 1, Ack: 1, Len: 6
- ▼ File Transfer Protocol (FTP)
 - ▼ QUIT\r\n
 - Request command: QUIT

Το **traceroute** χρησιμοποιεί το πρωτόκολλο **ICMP** (Internet Control Message Protocol) για να ανακαλύψει τη διαδρομή που ακολουθεί ένα IP πακέτο από τον τοπικό host προς ένα απομακρυσμένο host:

στέλνει μικρά πακέτα με αρχικό TTL=1, και το αυξάνει κατά 1 με κάθε αποστολή πακέτου μέχρι να φτάσει στον τελικό προορισμό. Κάθε φορά που λήγει το TTL, ο κόμβος στον οποίο λήγει, στέλνει πίσω ICMP message (type 11 – TTL-exceeded)

➔ μαθαίνουμε την ταυτότητα των ενδιάμεσων δρομολογητών

WireShark Traceroute Demo

Try it out!

- Ξεκινήστε το WireShark
- Ανοίξτε ένα παράθυρο με `command prompt`
- Επιλέξτε το interface για ανίχνευση
- Ξεκινήστε την ανίχνευση 
- Στο command prompt παράθυρο δώστε την εντολή:
`tracert www.acm.org` (windows) ή
`traceroute www.acm.org` (linux, Mac OS)
- Σταματήστε την ανίχνευση 

- Επιλέγουμε το πρώτο ICMP Echo Request μήνυμα

The image shows a Wireshark capture of network traffic. The top pane displays a list of captured packets. The bottom pane shows the detailed view of the selected packet (Frame 8), which is an ICMP Echo (ping) request.

Packets List:

No.	Time	Source	Destination	Protocol	Length	Info
4	5.363536	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
5	5.364799	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
6	5.864428	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
7	5.865461	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
8	6.163045	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20483/848, ttl=1 (no response found!)
9	6.176826	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
10	6.188629	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849, ttl=2 (no response found!)
11	6.202957	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
12	6.208597	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20995/850, ttl=3 (no response found!)
13	6.234505	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)

- Ethernet II, Src: ActiontecEle_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysGroup_da:af:73 (00:06:25:da:af:73)
- Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 84
 - Identification: 0x32d0 (13008)
 - 000. = Flags: 0x0
 - 0... = Reserved bit: Not set
 - .0.. = Don't fragment: Not set
 - ..0. = More fragments: Not set
 - ...0 0000 0000 0000 = Fragment Offset: 0
 - Time to Live: 1
 - Protocol: ICMP (1)
 - Header Checksum: 0x2d2c [validation disabled]
 - [Header checksum status: Unverified]
 - Source Address: 192.168.1.102
 - Destination Address: 128.59.23.100
- Internet Control Message Protocol

Packet Bytes:

Offset	Hex	ASCII
0000	00 06	
0010	00 54	
0020	17 64	
0030	aa aa	
0040	aa aa	
0050	aa aa	
0060	aa aa	

ip-ethereal-trace-1 | Packets: 380 · Displayed: 380 (100.0%)

▶ ποια είναι η IP διεύθυνση του υπολογιστή σας;

```
▼ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x32d0 (13008)
  ▼ 000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0... .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x2d2c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
```

μέσα στην επικεφαλίδα, ποιο ανώτερο πρωτόκολλο περιέχεται;

```
▼ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x32d0 (13008)
  ▼ 000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
  Protocol: ICMP (1)
  Header Checksum: 0x2d2c [validation disabled]
    [Header checksum status: Unverified]
  Source Address: 192.168.1.102
  Destination Address: 128.59.23.100
```

ποιο το μέγεθος (σε bytes) της IP επικεφαλίδας;
ποιο το μέγεθος του IP payload;

```
▼ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x32d0 (13008)
  ▼ 000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0... .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x2d2c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
```

payload: 64

έχει γίνει fragmentation; πως το καταλαβαίνουμε;

```
▼ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x32d0 (13008)
  ▼ 000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x2d2c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
```

Παρατηρήστε την αλληλουχία των ICMP πακέτων που έχουν σταλεί από τον υπολογιστή σας

- ποια πεδία του IP datagram αλλάζουν από το ένα datagram στο άλλο;

tracert με μέγεθος πακέτου 2000 bytes (για να αναγκάσουμε σε fragmentation)

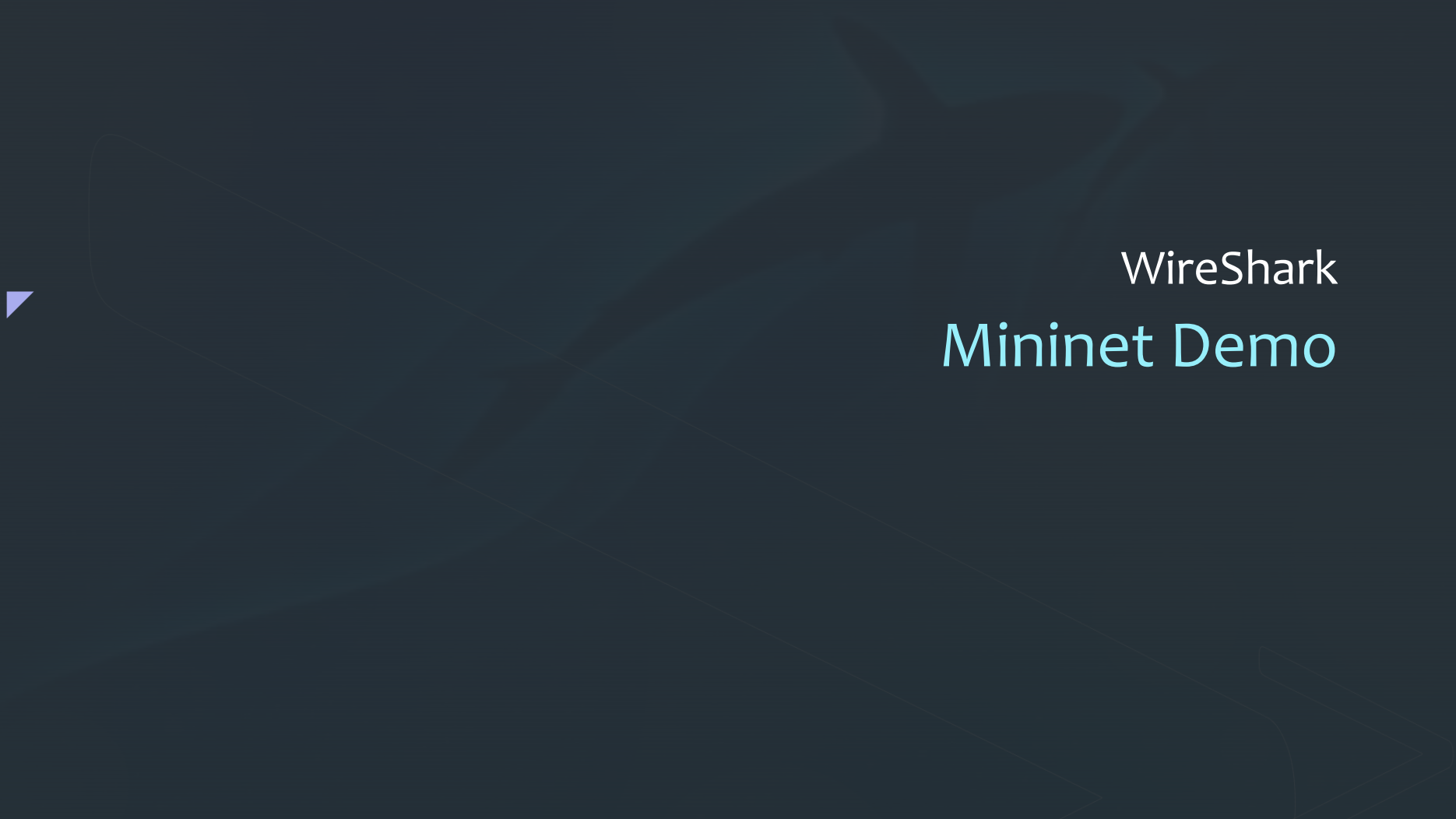
132	32.0670...	192.168.1.102	199.2.53.206	TCP	62 1483 → 631 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
133	33.4517...	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3307) [Reassembled in #134]
134	33.4524...	192.168.1.102	128.59.23.100	ICMP	562 Echo (ping) request id=0x0300, seq=33795/900, ttl=1 (no response found!)
135	33.4705...	10.216.228.1	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
136	33.4778...	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3308) [Reassembled in #137]
137	33.4785...	192.168.1.102	128.59.23.100	ICMP	562 Echo (ping) request id=0x0300, seq=34051/901, ttl=2 (no response found!)
138	33.4976...	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3309) [Reassembled in #139]
139	33.4983...	192.168.1.102	128.59.23.100	ICMP	562 Echo (ping) request id=0x0300, seq=34307/902, ttl=3 (no response found!)
140	33.5280...	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=330a) [Reassembled in #141]
141	33.5290...	192.168.1.102	128.59.23.100	ICMP	562 Echo (ping) request id=0x0300, seq=34563/903, ttl=4 (no response found!)
142	33.5379...	24.218.0.153	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
143	33.5552...	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=330b) [Reassembled in #144]
144	33.5558...	192.168.1.102	128.59.23.100	ICMP	562 Echo (ping) request id=0x0300, seq=34819/904, ttl=5 (no response found!)
145	33.5780...	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=330c) [Reassembled in #146]
146	33.5787...	192.168.1.102	128.59.23.100	ICMP	562 Echo (ping) request id=0x0300, seq=35075/905, ttl=6 (no response found!)

Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1500
Identification: 0x3307 (13063)
> 001. = Flags: 0x1, More fragments
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..1. = More fragments: Set
...0 0000 0000 0000 = Fragment Offset: 0
> Time to Live: 1
Protocol: ICMP (1)
Header Checksum: 0x076d [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.102
Destination Address: 128.59.23.100
[Reassembled IPv4 in frame: 134]

133	33.4517...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3307) [Reassembled in #134]
134	33.4524...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=33795/900, ttl=1 (no response found!)
135	33.4705...	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
136	33.4778...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3308) [Reassembled in #137]
137	33.4785...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=34051/901, ttl=2 (no response found!)
138	33.4976...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3309) [Reassembled in #139]
139	33.4983...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=34307/902, ttl=3 (no response found!)
140	33.5280...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=330a) [Reassembled in #141]
141	33.5290...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=34563/903, ttl=4 (no response found!)
142	33.5379...	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
143	33.5552...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=330b) [Reassembled in #144]
144	33.5558...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=34819/904, ttl=5 (no response found!)
145	33.5780...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=330c) [Reassembled in #146]
146	33.5787...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=35075/905, ttl=6 (no response found!)
147	33.5980...	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=330d) [Reassembled in #148]
148	33.5986...	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, seq=35331/906, ttl=7 (no response found!)

Identification: 0x3307 (13063)

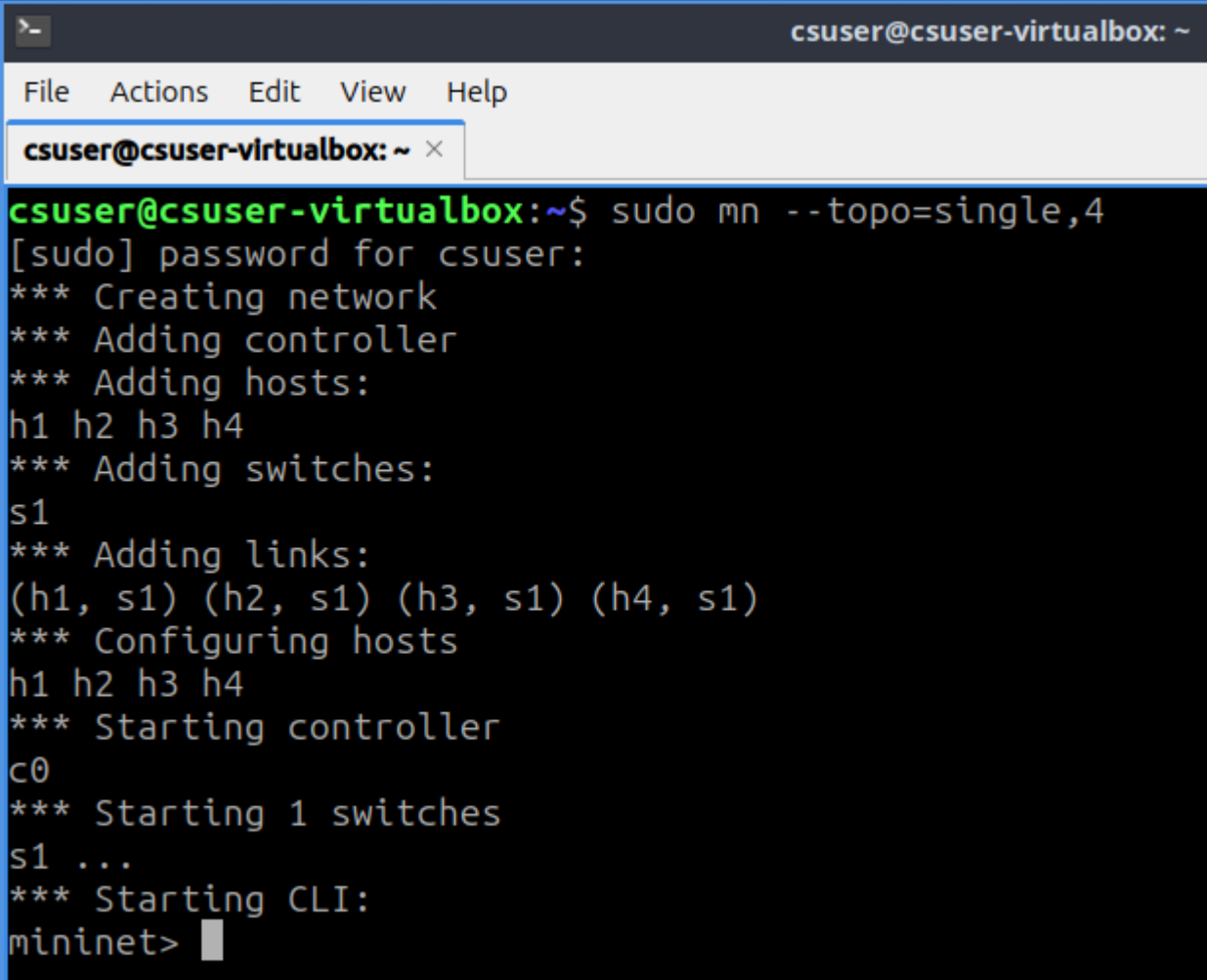
- 000. = Flags: 0x0
 - 0... = Reserved bit: Not set
 - .0.. = Don't fragment: Not set
 - ..0. = More fragments: Not set
 - ...0 0000 1011 1001 = **Fragment Offset: 1480**
- > Time to Live: 1
- Protocol: ICMP (1)
- Header Checksum: 0x2a6c [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 192.168.1.102
- Destination Address: 128.59.23.100
- > [2 IPv4 Fragments (2008 bytes): #133(1480), #134(528)]
 - [Frame: 133, payload: 0-1479 (1480 bytes)]
 - [Frame: 134, payload: 1480-2007 (528 bytes)]
 - [Fragment count: 2]
 - [Reassembled IPv4 length: 2008]
 - [Reassembled IPv4 data [truncated]: 0800c3c503008403373720aaaaa



Wireshark Mininet Demo

Έναρξη του Mininet

➤ `sudo mn --topo=single,4`

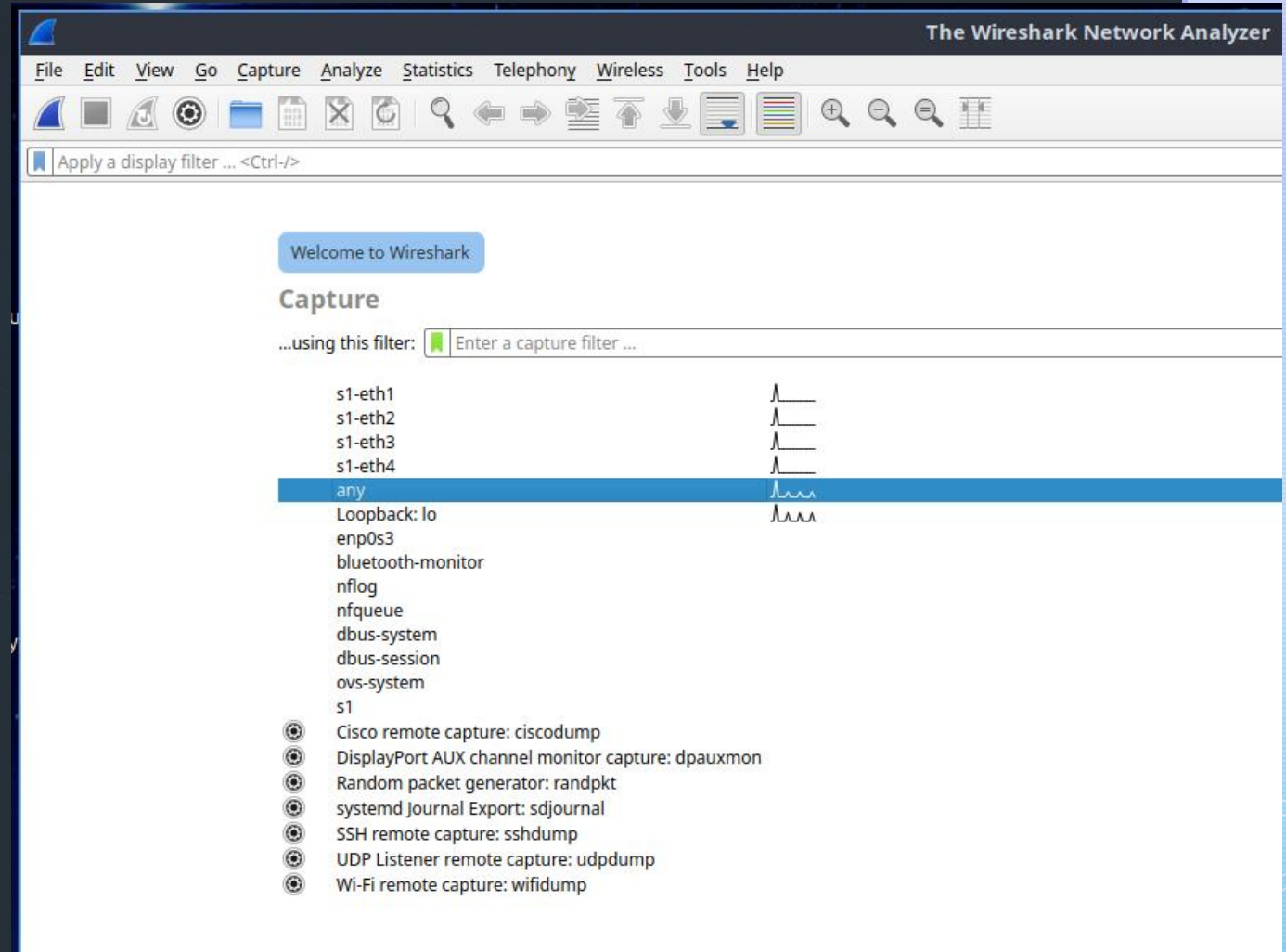


```
csuser@csuser-virtualbox: ~  
File Actions Edit View Help  
csuser@csuser-virtualbox: ~ x  
csuser@csuser-virtualbox:~$ sudo mn --topo=single,4  
[sudo] password for csuser:  
*** Creating network  
*** Adding controller  
*** Adding hosts:  
h1 h2 h3 h4  
*** Adding switches:  
s1  
*** Adding links:  
(h1, s1) (h2, s1) (h3, s1) (h4, s1)  
*** Configuring hosts  
h1 h2 h3 h4  
*** Starting controller  
c0  
*** Starting 1 switches  
s1 ...  
*** Starting CLI:  
mininet>
```

Έναρξη του Wireshark (χωριστό terminal)

➤ `sudo wireshark`

- Επιλέγω interface: any
- Ξεκινάω capture



mininet> pingall

```

mininet> pingall
*** Ping: testing ping reachability
h1 -> h2 h3 h4
h2 -> h1 h3 h4
h3 -> h1 h2 h4
h4 -> h1 h2 h3
*** Results: 0% dropped (12/1)
mininet>

```

*any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
23	12.719049434	10.0.0.1	10.0.0.2	ICMP	100	Echo (ping) request id=0x09cc, seq=1/256, ttl=64 (no response found!)
28	12.719865469	10.0.0.1	10.0.0.2	ICMP	100	Echo (ping) request id=0x09cc, seq=1/256, ttl=64 (reply in 29)
29	12.719891242	10.0.0.2	10.0.0.1	ICMP	100	Echo (ping) reply id=0x09cc, seq=1/256, ttl=64 (request in 28)
34	12.720967910	10.0.0.2	10.0.0.1	ICMP	100	Echo (ping) reply id=0x09cc, seq=1/256, ttl=64
47	12.734443540	10.0.0.1	10.0.0.3	ICMP	100	Echo (ping) request id=0x09cd, seq=1/256, ttl=64 (no response found!)
52	12.735409060	10.0.0.1	10.0.0.3	ICMP	100	Echo (ping) request id=0x09cd, seq=1/256, ttl=64 (reply in 53)
53	12.735430606	10.0.0.3	10.0.0.1	ICMP	100	Echo (ping) reply id=0x09cd, seq=1/256, ttl=64 (request in 52)
58	12.735949721	10.0.0.3	10.0.0.1	ICMP	100	Echo (ping) reply id=0x09cd, seq=1/256, ttl=64
71	12.740819209	10.0.0.1	10.0.0.4	ICMP	100	Echo (ping) request id=0x09ce, seq=1/256, ttl=64 (no response found!)
76	12.741501491	10.0.0.1	10.0.0.4	ICMP	100	Echo (ping) request id=0x09ce, seq=1/256, ttl=64 (reply in 77)
77	12.741523712	10.0.0.4	10.0.0.1	ICMP	100	Echo (ping) reply id=0x09ce, seq=1/256, ttl=64 (request in 76)
82	12.742067482	10.0.0.4	10.0.0.1	ICMP	100	Echo (ping) reply id=0x09ce, seq=1/256, ttl=64
83	12.746391618	10.0.0.2	10.0.0.1	ICMP	100	Echo (ping) request id=0x09cf, seq=1/256, ttl=64 (no response found!)
88	12.746740180	10.0.0.2	10.0.0.1	ICMP	100	Echo (ping) request id=0x09cf, seq=1/256, ttl=64 (reply in 89)
89	12.746755820	10.0.0.1	10.0.0.2	ICMP	100	Echo (ping) reply id=0x09cf, seq=1/256, ttl=64 (request in 88)
94	12.747377160	10.0.0.1	10.0.0.2	ICMP	100	Echo (ping) reply id=0x09cf, seq=1/256, ttl=64
107	12.751447773	10.0.0.2	10.0.0.3	ICMP	100	Echo (ping) request id=0x09d0, seq=1/256, ttl=64 (no response found!)
112	12.752052007	10.0.0.2	10.0.0.3	ICMP	100	Echo (ping) request id=0x09d0, seq=1/256, ttl=64 (reply in 113)
113	12.752068606	10.0.0.3	10.0.0.2	ICMP	100	Echo (ping) reply id=0x09d0, seq=1/256, ttl=64 (request in 112)
118	12.753363006	10.0.0.3	10.0.0.2	ICMP	100	Echo (ping) reply id=0x09d0, seq=1/256, ttl=64
131	12.757944176	10.0.0.2	10.0.0.4	ICMP	100	Echo (ping) request id=0x09d1, seq=1/256, ttl=64 (no response found!)
136	12.758522106	10.0.0.2	10.0.0.4	ICMP	100	Echo (ping) request id=0x09d1, seq=1/256, ttl=64 (reply in 137)
137	12.758544257	10.0.0.4	10.0.0.2	ICMP	100	Echo (ping) reply id=0x09d1, seq=1/256, ttl=64 (request in 136)
142	12.758906728	10.0.0.4	10.0.0.2	ICMP	100	Echo (ping) reply id=0x09d1, seq=1/256, ttl=64
143	12.762671038	10.0.0.3	10.0.0.1	ICMP	100	Echo (ping) request id=0x09d2, seq=1/256, ttl=64 (no response found!)
148	12.763412673	10.0.0.3	10.0.0.1	ICMP	100	Echo (ping) request id=0x09d2, seq=1/256, ttl=64 (reply in 149)
149	12.763428793	10.0.0.1	10.0.0.3	ICMP	100	Echo (ping) reply id=0x09d2, seq=1/256, ttl=64 (request in 148)
154	12.764376733	10.0.0.1	10.0.0.3	ICMP	100	Echo (ping) reply id=0x09d2, seq=1/256, ttl=64
155	12.767641238	10.0.0.3	10.0.0.2	ICMP	100	Echo (ping) request id=0x09d3, seq=1/256, ttl=64 (no response found!)
160	12.768067965	10.0.0.3	10.0.0.2	ICMP	100	Echo (ping) request id=0x09d3, seq=1/256, ttl=64 (reply in 161)
161	12.768085566	10.0.0.2	10.0.0.3	ICMP	100	Echo (ping) reply id=0x09d3, seq=1/256, ttl=64 (request in 160)
166	12.768674430	10.0.0.2	10.0.0.3	ICMP	100	Echo (ping) reply id=0x09d3, seq=1/256, ttl=64

Frame 23: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface
Linux cooked capture v1
Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.2
Internet Control Message Protocol

0000 00 03 00 01 00 06 26 40 3a a5 bb 40 00 00 08 00
0010 45 00 00 54 fe 47 40 00 40 01 28 5f 0a 00 00 00
0020 0a 00 00 02 08 00 2d 74 09 cc 00 01 bd 99 62 6
0030 00 00 00 00 d9 ea 00 00 00 00 00 11 12 1
0040 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 2
0050 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 3
0060 34 35 36 37